Office of the Auditor General of Ontario
Bureau de la vérificatrice générale de l'Ontario

Volume 1, Chapter 3.13—Technology Systems (IT) and Cybersecurity at Ontario Lottery and Gaming Corporation

2019 Value-for-Money Audit

Why We Did This Audit

- Ontario Lottery and Gaming (OLG) contributed about 45% of the total $5.47 billion in non-tax revenue generated in 2018/19 by provincial government business enterprises, which also include the Liquor Control Board, Ontario Power Generation, Hydro One and the Ontario Cannabis Retail Corporation.
- An assessment of IT systems at OLG, vendor performance review and cybersecurity had not been performed by our Office.

Why It Matters

- Cybersecurity is a critical measure to protect OLG from cyberattacks, privacy breaches, reputational damage, and the destruction of critical information and IT infrastructure.
- Interruptions to OLG's businesses can negatively affect not only their customers' experience but also potentially reduce provincial revenue.

What We Found

- OLG has not always kept up to date with its testing for security vulnerabilities on its IT systems. Although OLG conducts regular vulnerability assessments, OLG has not regularly performed security tests such as penetration testing to further identify cybersecurity vulnerabilities. In November 2018, OLG's Internet gaming (iGaming) IT system was attacked by a hacker, making it unavailable for 16 hours and impacting customer experience.
- Seven OLG staff have access to unencrypted confidential customer information. Personal information of OLG customers is encrypted to prevent external access to it; however, the seven OLG employees have access to the information in an unencrypted form, which increases the risk of customers' personal information being read for inappropriate purposes. In addition, we found that two casinos we visited do not comply with OLG information security standards and do not encrypt OLG customer data within their IT systems.
- We found that OLG does not follow industry best practices of reviewing the source code (the list of human-readable instructions that a programmer writes) for cybersecurity weaknesses within critical IT systems for its lottery, iGaming and casino operations.
- Although disaster recovery strategies are developed and tested for IT systems for each individual line of business, we noted that OLG does not have a comprehensive disaster recovery strategy that incorporates all IT systems cohesively, even after it had a significant event occur that should have triggered OLG to prepare one.
- Critical IT performance indicators are not always incorporated in the service-level agreement with IT vendors. Three out of the 10 service-level agreements we reviewed did not include key IT performance indicators. Depending on the service-level agreement, one or more critical performance indicators, such as system availability, service outages, incident resolution or response times, were not included. This impacts, in various degrees, measurement of the customer experience, and, potentially, revenue and business operations.
- Certain IT vendors are underperforming and not held accountable for meeting performance targets. OLG does not consistently review the performance of all IT vendors against their service-level agreement and take remedial action where appropriate, such as imposing fines as per their service-level agreement. We found examples where IT vendors' performance was not reviewed by OLG.
- OLG has initiated major IT projects across its various lines of its business. OLG implemented 33 IT projects within budget; however, the remaining 11 were over budget, which account for almost half of all IT project expenses over the last five years ($91 million sampled over a total of $232 million spent), and had delays and cost overruns of over $10 million.

..../2

Conclusions

- There are opportunities to strengthen cybersecurity practices in OLG IT systems. OLG has not regularly performed security tests such as penetration testing for its lottery and iGaming lines of business to further identify potential vulnerabilities.
- There are opportunities to strengthen the protection of customer information in certain gaming IT systems in OLG and two casinos.
- OLG needs to improve its oversight of the IT vendors that provide IT services. This is especially significant because of how heavily OLG relies on these IT vendors. OLG's IT contracts do not always contain the necessary performance requirements needed to ensure operations are delivered efficiently.

Read the audit report at www.auditor.on.ca